

## REMARKS

A number of aspects of the specification where objected to in paragraphs 3-5 of the above Office Action. These objections have been addressed by the above amendments.

The drawings stand objected to as has not being labeled appropriately. Appropriate corrections are indicated on the attached red-line copy of Figure 1. Claim 2 stands objected to because of an informality. Claim 2 has been amended as indicated herein to address this objection.

Claims 1-10 stand objected to under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. This objection is addressed by the proposed amendments indicated herein.

Claims 1-4 and 6-8 stand rejected under 35 USC 102 (e) as being anticipated by U.S. patent number 6,089,460 (the '460 patent). Applicant respectfully traverses this rejection for the reasons set out below.

Claim 1, as amended, includes the following limitations:

*"a number of secure devices, each of said secure devices comprising a chip with logic circuitry having a function in providing authorization to the security system, characterized in that in at least groups of said secure devices, the chip of a secure device is provided with a unique chip layout".* (Emphasis added).

Regarding the rejection of claims 1, 6 and 8 on grounds of lack of novelty, it is observed that the '460 patent discloses a security system comprising an IC card. However, the publication relates to the IC card, and not to the system, in that the '460

patent merely discloses how one specific IC card is programmed. The '460 patent does not disclose a system comprising a number of secure devices. Crucially, it does not disclose a system wherein, in at least groups of the secure devices, the chip of a secure device is provided with a unique chip layout.

Although the IC card disclosed in the '460 patent comprises an FPGA, it is provided for a different purpose. The reasons for using an FPGA are set out in column 10, line 65 a.f. They are firstly to prevent someone using a microscope to study the layout of the logic (see also column 4, lines 27-33), secondly, to perform the (de-) ciphering at high speed, and thirdly to keep the CPU free to execute other processing between ciphering and deciphering. These issues are at best remotely related to the problem of preventing a pirate who has cracked one card from cracking another card in the system. Preventing such an attack, wherein appropriate probe points can be determined, for example, is not achieved by just providing the IC card with an FPGA. It requires that, in at least groups of the secure devices, the chip of a secure device is provided with a unique chip layout.

The prior art devices mentioned in column 1 of the '460 patent comprise an EEPROM storing a ciphering program, but neither this EEPROM nor the CPU for controlling the ciphering function has a unique layout. The disclosed systems all rely on unique data, stored in a circuit that appears to have the same layout for each device. They are thus all vulnerable to the type of attack described on page 1 of the present application.

In summary, it is submitted that the present invention as defined in independent claims 1, 6 and 8, is not disclosed in the '460 patent.

It is noted that the '460 patent, taken in combination with any of the other two documents cited in the Office Action, does not fully disclose the subject matter of presently pending claim 1.

It is observed that US patent number 4,924,075 (the '075 patent) discloses a smart IC card. The IC card includes a timepiece circuit. As in the '460 patent, no mention is made of a security system comprising a number of secure devices, wherein in at least groups of said secure devices, the chip of a secure device is provided with a unique chip layout. The '075 patent is concerned with conserving the battery life of an IC card as much as possible, and enabling the card to operate in its timepiece mode without requiring an extra operation (column2, lines 1-6). Since the transaction mode of the disclosed IC card is not described in any detail, it is submitted that the '075 patent is not relevant to an assessment of the novelty or obviousness of the present invention.

The third cited publication, US patent number 5,594,657(the '657 patent) discloses a system for synthesizing field programmable gate array implementations from high-level circuit descriptions. It does not relate to a security system comprising a number of secure devices. Rather, it relates to a system that uses advanced optimization techniques to produce efficient FPGA implementations. This teaches away from the present invention, since the system is concerned with finding the single chip layout that is an optimum in terms of efficiency. It stands to reason, that where a number of FPGA circuits is to be provided with the same logic, this single chip layout will be used for all of them.

In summary, none of the cited documents, when taken alone or in combination fully discloses the present invention as described in claims 1, 6 and 8. Of the three cited documents, only the '460 patent relates to a security system. The other two documents do not relate to a security system. In addition, neither the '075 patent nor the '657 patent disclose a number of secure devices comprising a chip wherein, in at least groups of the secure devices, the chip of a secure device is provided with a unique chip layout. The problem posed in the introduction of the present application, namely that once a smart card has been cracked for the first time, any second attack is relatively easy, is not addressed by any of the three documents. The present invention recognizes the

existence of this problem and provides a solution for it. Since this solution cannot be found in the prior art, it is submitted that the invention comprises an inventive step.

Concluding, it is hereby submitted that claims 1, 6 and 8 are allowable, since the invention defined thereby is both novel and comprises an inventive step.

The other claims, being dependent on one of claims 1, 6 and 8, are likewise allowable.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicants hereby request such an extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Dated: 12 / 26 / 2001



André L. Marais

Reg. No.: 48,095

12400 Wilshire Blvd.  
Seventh Floor  
Los Angeles, CA 90025  
(408) 720-8300

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

**Please amend the claims as follows:**

1. (Amended) Security system for [preventing unauthorized use, entrance or the like, comprising] checking authorization, the system including a number of secure devices, each of said secure devices comprising a chip with logic circuitry having a function in providing authorization to the security system, characterized in that in at least [a part] groups of said secure devices, the chip of a secure device is provided with a unique chip layout.

2. (Amended) Security system according to claim 1, wherein at least said logic circuitry of the chips of said part of the secure devices is implemented in Field Programmable Gate Array FPGA technology, wherein the layout is programmed in the FPGA circuitry [either] in at least one of a volatile [or] and a non-volatile manner.

3. (Unamended) Security system according to claim 2, wherein the logic circuitry of each secure device chip is provided in a secure cell of the chip.

4. (Amended) Security system according to claim 1, wherein the complete secure device chip is implemented in FPGA technology, wherein the layout is programmed in the chip [either] in at least one of a volatile [or] and a non-volatile manner.

5. (Amended) Security system according to claim 2 wherein at least one of the logic circuitry [or] and the entire chip is made as a volatile programmable FPGA, wherein the FPGA program is stored in a battery powered RAM.

6. (Amended) A set of secure devices [to be used in] for a security system according to claim 1, wherein each of said secure devices comprises a chip with logic circuitry having a function in providing authorization to the holder of a secure device, wherein in at least [a part] groups of said secure devices, the chip of each secure device is provided with a unique chip layout.

7. (Amended) A set according to claim 6, wherein at least said logic circuitry of the chips of said part of the secure devices is implemented in FPGA technology, wherein the layout is programmed in the FPGA circuitry [either] in at least one of a volatile [or] and a non-volatile manner.

8. (Unamended) Method for manufacturing a secure device for a security system according claim 1, wherein secure devices with a chip are used, said chips having logic circuitry having a function in providing authorization to the security system, wherein in at least a part of said secure devices, the chip of a secure device is provided with a unique chip layout.

9. (Amended) Method according to claim 8, wherein chips with logic circuitry in FPGA technology are used, said method comprising [the steps of] programming a unique information in the logic circuitry [by means of] utilizing a synthesis tool and a layout tool, wherein for each secure device of said part of secure devices, a variation factor is introduced in at least one of the synthesis tool and the layout tool, thereby providing a unique circuit layout.

10. (Unamended) Method according to claim 9, wherein the synthesis tool is provided with input information compiled from a high level language code, wherein a variation factor is introduced in at least one of the compilation step of the high level language code, the synthesis tool and the layout tool.

### ABSTRACT OF THE DISCLOSURE

A security system for preventing unauthorized use, entrance or the like, comprises a number of secure devices, each of the secure devices comprising a chip with logic circuitry having a function in providing authorization to the security system. In at least a part of the secure devices to chip of the secure device is provided with a unique chip layout.

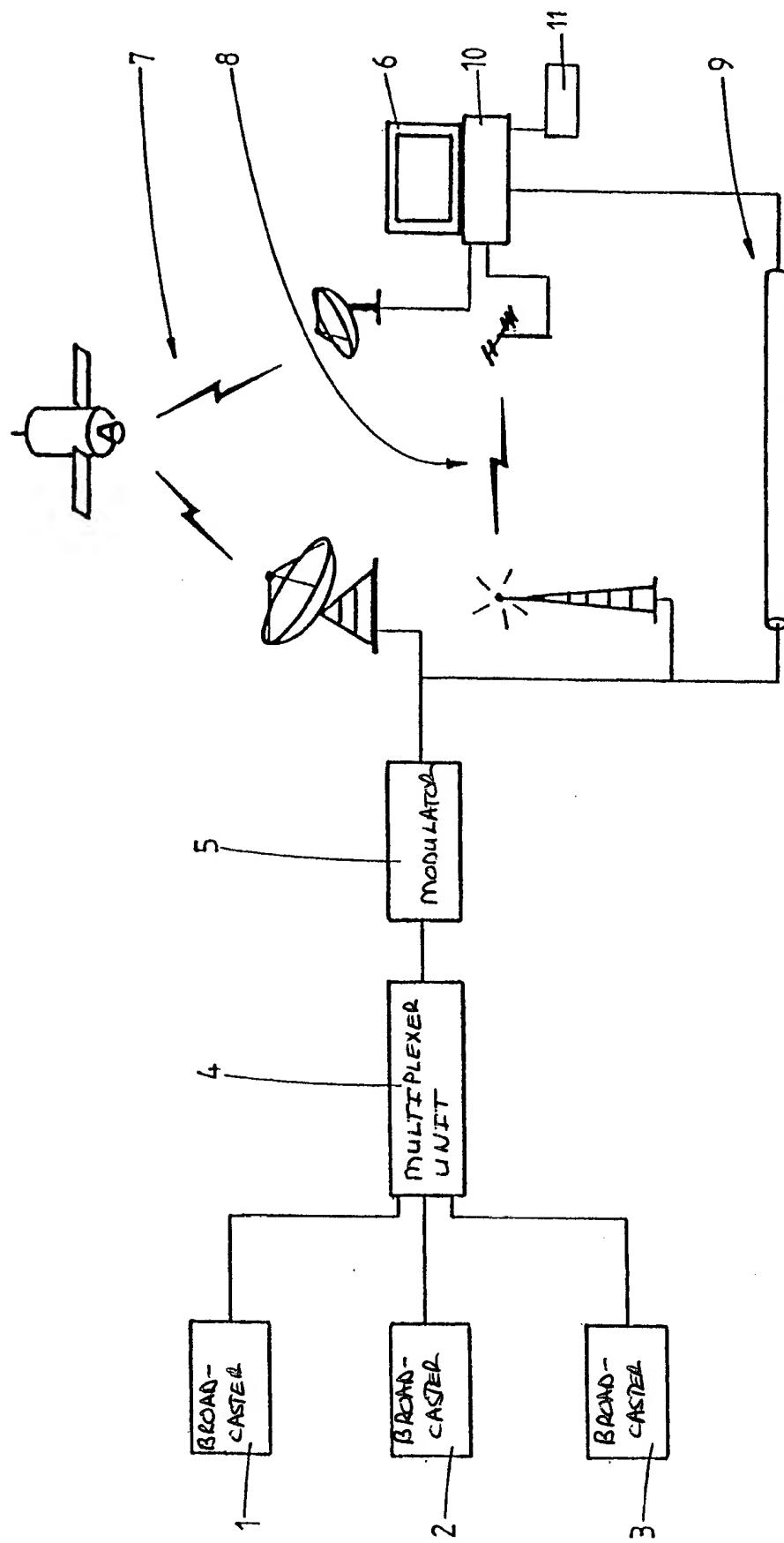


fig.1